Claims 1 - 26 have been cancelled without prejudice or disclaimer. Claims 27 - 75 have been voluntarily added to round out the scope of the invention.

Applicant respectfully submits that no new matter has been added and the amendments made above are not to create estoppel that limits the scope of the claims.

Attached hereto is a marked-up version of the changes made to the specification by the current amendment. The attached page is captioned **"Version With Markings To Show Changes Made"**.

Attached hereto is a clean version of the new claims added by the current amendment as per 37 CFR § 1.121. The first attached page is captioned **"Clean Version Of Claims For Scanning Per 37 CFR § 1.121"**.

Applicant asserts that the present invention is new, non-obvious and useful. Entry of this Amendment, prompt consideration and allowance of the claims is respectfully requested.

If the Examiner has any questions or comments as to the form, content, or entry of this paper, the Examiner is requested to contact the undersigned at the address and telephone number below.

Respectfully submitted,

Adele Marcus
Attorney for Applicant(s)
Registration No. 47, 769

Dated: August 16, 2001

Eitan, Pearl, Latzer & Cohen-Zedek
One Crystal Park, Suite 210
2011 Crystal Drive
Arlington, VA 22202-3709, U.S.A.
Telephone No.: (703) 486-0600
Facsimile No.: (703) 486-0800

Version With Markings To Show Changes Made”

In the specification:

Paragraph beginning at page 17, line 3, has been amended as follows:

NAP 16, as mentioned hereinabove, has access to user information database 22. User [Information] information database 22 is a database external to the invention and may be any known data collection or database system known in the art. It may provide enhanced user information, for example, personal details related to a given user ID, billing information, technical details, information about past logins, or customer care cases. In addition, the system may also have access to a user information database 22 known as a reverse telephone directory. A reverse telephone directory may associate a given telephone number with information about its owner and its location. User information database 22 may be used in identifying user 10.

Clean Version Of Claims For Scanning Per 37 CFR § 1.121

27. A method for the identification of a user, said method comprising:

receiving by at least one network access provider (NAP) through which a user is engaged in a communication session with a service provider, a request from said service provider to identify said user;

said at least one NAP extracting information associated with said communication session; and

said at least one NAP sending a response based on said information to said service provider.

28. The method according to claim 27, wherein said receiving comprises receiving said request via at least one identification switch.

29. The method according to claim 27, wherein said extracting is performed by the NAP servicing said user.

30. The method according to claim 27, wherein said request comprises at least one session identifier of said communication session.

31. The method according to claim 30, wherein said at least one session identifier comprises at least one network address used by said user.

32. The method according to claim 27, wherein said extracting comprises:

second extracting at least one network address used by said user.

33. The method according to claim 32, wherein said second extracting comprises at least one of:

instructing a device being used by said user to connect to an address extraction module of said NAP via an alternative service or port not associated with a proxy server;

configuring said device not to connect to said proxy server when connecting to a specific network address;

opening a direct connection between an application sent to said device and said address extraction module;

using a proxy plug-in;

installing a network sniffer between said device and said proxy server;

installing network extraction module between said device and said proxy server;

accepting as correct a user network address reported by said proxy server; and

configuring said device to echo back a secret sent to said device and verifying that the sent secret and the received secret are identical.

34. The method according to claim 27, wherein said extracting comprises:

retrieving data from a group of databases including an online session database and a user information database, said online session database and said user information database being in communication with said at least one NAP.

35. The method according to claim 27, wherein said sending comprises:

reporting information associated with said user associated with said communication session.

36. The method according to claim 35, wherein said sending comprises:

sending to said service provider information associated with said user in a previous request.

37. The method according to claim 27, wherein sending comprises:

verifying the information items provided in said identification request; and

sending a match report noting the similarity between said information associated with said communication session and said information items provided in said identification request.

38. The method according to claim 27, wherein said sending comprises:

sending a virtual identification (ID) for said user to said service provider.

39. The method according to claim 27, further comprising:

determining the identity of the NAP currently handling said communication session; and

forwarding said identification request to the identification module of said NAP currently handling said communication session.

40. The method according to claim 39, wherein said sending is performed only by the NAP currently handling said communication session.

41. The method according to claim 39, wherein said determining comprises:

maintaining a look-up table of network addresses associated with a plurality of NAPs; and

determining the identity of said at least one NAP by reference to said look-up table.

42. The method according to claim 41, wherein said maintaining comprises manually updating said look-up table whenever network address assignments change.

43. The method according to claim 41, wherein said maintaining comprises updating said look-up table from said identification module of said at least one NAP currently handling said communication session based on information reported from an access system.

44. The method according to claim 41, wherein said maintaining comprises constructing said look-up table from existing network address assignment databases.

45. The method according to claim 39, wherein said determining comprises:

preconfiguring said at least one NAP servicing said user to intercept a user request for a specific resource; and

causing the device being used by said user to send a request to said specific resource so that only the NAP currently handling said communication session will receive said request thereby determining said NAP currently handling said communication session.

46. The method according to claim 27, wherein said network is selected from at least one of the group consisting of:

an Internet network;

a wireless data network;

a cellular data network; and

a CATV-based data network.

47. The method according to claim 27, wherein said user is connected to said NAP over a link selected from among the group consisting of:

a telephone link;

a cellular telephone link;

a Wireless link;

a data over CATV link;

a satellite link;

an xDSL link; and

a link over another data network.

48. A method according to claim 27, wherein said information is selected from among the group consisting of:

an account identifier of said user associated with said communication session at said NAP;

information associated with said account identifier;

an identifier of a link between said user and said NAP; and

information associated with said link identifier.

49. A method for identifying a user, said method comprising:

a service provider sending a request to identify said user to at least one network access provider through which said user is engaged in a communication session with said service provider, said request including an identifier of said communication session; and

a service provider receiving an identification response.

50. The method according to claim 49, wherein said sending comprises sending the request via at least one identification switch.

51. The method according to claim 49, wherein said identifier is a network address of said user.

52. A method for identifying a user, said method comprising:

an identification switch receiving from a service provider a request to identify said user engaged in a communication session through a NAP with said service provider;

an identification switch sending said request to at least one network access provider for further processing;

an identification switch receiving information associated with said communication session; and sending an identification response to said service provider.

53. The method according to claim 52, further comprising:

determining the identity of the NAP currently handling said communication session; and

forwarding said request to the identification module of said NAP currently handling said communication session.

54. The method according to claim 53, wherein said determining comprises:

maintaining a look-up table of network addresses associated with a plurality of NAPs; and

determining the identity of said at least one NAP by reference to said look-up table.

55. The method according to claim 54, wherein said maintaining comprises manually updating said look-up table whenever network address assignments change.

56. The method according to claim 54, wherein said maintaining comprises updating said look-up table from said identification module of said at least one NAP currently handling said communication session based on information reported from an access system.

57. The method according to claim 54, wherein said maintaining comprises constructing said look-up table from existing network address assignment databases.

58. The method according to claim 53, wherein said determining comprises:

preconfiguring said at least one NAP servicing said user to intercept a user request for a specific resource; and

causing the device being used by said user to send a request to said specific resource so that only the NAP currently handling said communication session will receive said request thereby determining said NAP currently handling said communication session.

59. A method according to claim 52, wherein said information is selected from among the group consisting of:

an account identifier of said user associated with said communication session at said NAP;

information associated with said account identifier;

an identifier of a link between said user and said NAP; and

information associated with said link identifier.

60. A method for determining the NAP currently handling a communication session over a network between a user and a service provider, the method comprising:

maintaining a look-up table of network addresses associated with a plurality of NAPs; and

determining the identity of said NAP by reference to said look-up table.

61. The method according to claim 60, wherein said maintaining comprises updating said look-up table manually whenever network address assignments change.

62. The method according to claim 60, wherein said maintaining comprises updating said look-up table from the identification module of said NAP based on information reported from an access system.

63. The method according to claim 60, wherein said maintaining comprises constructing said look-up table from existing network address assignment databases.

64. A method for determining the NAP currently handling a communication session over a network between a user and a service provider, the method comprising the steps of:

preconfiguring said NAP to intercept a user request for a specific resource; and

causing the device being used by said user to send a request to said specific resource so that only the NAP currently handling said communication session will receive said request thereby determining said NAP currently handling said communication session.

65. A method for determining the network address of a user, said method comprising at least one of:

instructing a device being used by said user in a communication session with a service provider over a network through a network access provider to connect to an address extraction module of said NAP via an alternative service or port not associated with a proxy server;

configuring said device not to connect to said proxy server when connecting to a specific network address;

opening a direct connection between an application sent to said device and said address extraction module;

using a proxy plug-in;

installing a network sniffer between said device and said proxy server;

installing network extraction module between said device and said proxy server;

accepting a user network address reported by said proxy server; and

configuring said device to echo back a secret sent to said device and verifying that the sent secret and the received secret are identical.

66. A system for acquiring at least one user identifier of a user of a network, said system comprising:

a service provider in communication with said user; and

at least one network access provider (NAP) in communication with said service provider and said user; said at least one NAP comprising:

a NAP identification module comprising:

a controller; and

an address extractor in communication with said controller; and

an access system in communication with said address extractor.

67. The system according to claim 66, further comprising at least one online session database in communication with said controller and said access system, said at least one online session database containing at least information associating said at least one user identifier with the network address being used by said user.

68. The system according to claim 66, further comprising an identification switch in communication with said at least one NAP and said service provider.

69. The system according to claim 66, further comprising at least one user information database, in communication with said controller.

70. The system according to claim 69, wherein said at least one user information database comprises at least one of a group of databases containing data including

personal details related to said user, billing information, information about past user logins, and a reverse telephone directory.

71. The system according to claim 68, wherein said address extractor is located in at least one of said at least one identification switch.

72. The system according to claim 68, wherein said address extractor is located at said service provider.

73. A method for creating an online session database by device, said method comprising:

externally monitoring login and logout events at an access system;

saving session information upon login; and

removing said session information upon logout.

74. The method according to claim 73, wherein said monitoring is done by a network sniffer.

75. The method according to claim 73, wherein said monitoring is done by reading server log files.